

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-323351

(43)Date of publication of application : 14.11.2003

(51)Int.Cl. G06F 12/14
G11B 20/10
G11B 20/12
G11B 27/00
H04L 9/08
H04L 9/32

(21)Application number : 2003-050043 (71)Applicant : MATSUSHITA ELECTRIC IND
CO LTD

(22)Date of filing : 26.02.2003 (72)Inventor : MIYAMOTO HARUTOSHI

(30)Priority

Priority number : 2002050963 Priority date : 27.02.2002 Priority country : JP

(54) COPYRIGHT MANAGEMENT SYSTEMCOPYRIGHT MANAGEMENT
METHODHOST DEVICEPROGRAM AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a copyright protection system and a copyright protection method that are easy for users to use a host device therefor a program therefor and a recording medium carrying the program.

SOLUTION: The host device encrypts prescribed contents by a prescribed encryption methodselects a specific reproducer 5 in dependence on the number of reproducers 5 preauthorized for reproductionand sends decryption information such as a decryption key for decrypting the encrypted contents 6 to the selected specific reproducer 5.

CLAIMS

[Claim(s)]

[Claim 1]A host device which sends decoding information for choosing specific playback equipment and decrypting said enciphered contents to said specific selected

playback equipment according to the number of playback equipment to which reproduction was permitted while enciphering predetermined contents with a predetermined encryption method.

[Claim 2]The host device according to claim 1 further provided with a selection indication means for directing said selection.

[Claim 3]The host device according to claim 1 with which said encryption uses host ID peculiar to said host deviceand apparatus ID and said host ID of said specific playback equipment are contained in said decoding information.

[Claim 4]The host device according to claim 1 which said predetermined contents and information on said number are enciphered from a distributing serverand is distributed.

[Claim 5]Apparatus ID which host ID which contents enciphered by a host device haveand host ID contained in said decoding information are in agreementand is contained in said decoding informationOn condition that peculiar apparatus ID is in agreementare said enciphered contents playback equipment to reproduceand said host deviceWhile enciphering predetermined contents using peculiar host IDPlayback equipment which chooses specific playback equipment and sends decoding information in which apparatus ID and said host ID of said specific playback equipment for decrypting said enciphered contents to said specific selected playback equipment are contained according to the number of playback equipment to which reproduction was permitted.

[Claim 6]The playback equipment according to claim 5 by which said playback equipment is not connected to the Internet.

[Claim 7]A distributing server which distributes predetermined contentsand a host device which enciphers predetermined contents with a predetermined encryption methodHave playback equipment which reproduces said enciphered contentsand said host deviceSaid specific playback equipment is chosen according to the number of playback equipment to which reproduction was permittedA copyright management system which sends decoding information for decrypting said enciphered contents to said specific selected playback equipment and by which said playback equipment reproduces said enciphered contents using said sent decoding information.

[Claim 8]A distributing server which distributes predetermined contentsand a host device which enciphers said predetermined contents with a predetermined encryption methodAre a copyright management system provided with playback equipment which reproduces said enciphered contents the used copyright management methodand said host deviceSaid specific playback equipment is chosen according to the number of said playback equipment to which reproduction was permittedA copyright management method that send decoding information for decrypting said enciphered contents to said specific selected playback equipmentand said playback equipment reproduces said enciphered contents using said sent decoding information.

[Claim 9]A program for operating a host device which enciphers predetermined contents of the copyright management system according to claim 7 with a

predetermined encryption method and playback equipment which reproduces said enciphered contents as a computer.

[Claim 10] It is the recording medium which made the program according to claim 9 support and is an available recording medium with a computer.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the copyright management system and the copyright management method of performing license management of the copyright of contents, its host device, its program, and the recording medium of the program.

[0002]

[Description of the Prior Art] In recent years, the music form reproduced from the sound source of origin not only like CD-DA but mp3 (mpeg audio layer 3) is widely used for the user. However, since the method of copyright management is not established to mp3, it has been a big problem for an owner of a copyright and the means which is going to solve this is proposed. The method of copyright management is examined also about digital contents such as not only music but an image and a picture. For example, the system called DRM (Digital Right Management) in the copyright management of music compression technology called WMA (Windows (registered trademark) Media Audio) used on a personal computer is adopted. This is a system with which peculiar ID of the enciphered equipment is needed for a decoding of the enciphered music.

Spread of an illegal copy can be prevented by limiting an enciphering device and playback equipment to the same equipment.

The system which protects the copyright of delivery information is proposed also in the information distribution system which targeted sized terminals such as a cellular phone (for example, refer to patent documents 1). The information distributed from the distributing server and peculiar ID of the cellular phone of a distribution destination are registered into the management data base on a server and it has become the structure which can reproduce information only with the registered cellular phone.

[0003]

[Patent documents 1] JP2001-78266A [0004]

[Problem to be solved by the invention] However, since it will be the requisite that each equipment can access the server on a network, it is not realizable with the playback equipment on condition of network connection etc.

[0005] Ways the playback equipment which cannot access a network directly performs license management of copyright include the method shown in drawing 13. In drawing

13101 is an electronic music distribution (EMD) server.

The media in which 102 has an Internet line 103 has users' personal computer and 104 has peculiar ID for example an SD card (Secure Digital card) and 105 are the general-purpose playback apparatus 105 which is not connected to the Internet line.

[0006] Here check-in is transmitted and received and data is transmitted between the personal computer 103 and SD card 104 and received by a check-out system. While check-in of data and check-out manage the number of times of a copy of data it says transmitting and receiving data between a personal computer and an external instrument and media. Check-out means transmitting data to an external instrument and media from a personal computer. In this case when data has restricted frequency of check-out (copy) the check-out exceeding restricted frequency cannot be performed. Check-in means returning an external instrument and the data transmitted to media to the personal computer of the source from a personal computer so that it may not remain in those external instruments and media. The data in which he was checked out in this case can be returned only to the personal computer of the source. However he can check out again the data returned to the personal computer by check-in.

[0007] According to this method by treating contents together with peculiar ID of SD card 104 which is media the original copy and duplicate of contents are distinguished and copyright management is performed. The illegal copy of data is prevented by specifically checking out the data of contents only to attested SD card 104. That is a user downloads contents data with users' personal computer 103 via Internet line 102 from EMD server 101. By inserting SD card 104 in the personal computer 103 the personal computer 103 checks that predetermined ID with which SD card 104 is attested beforehand is given. The personal computer 103 checks out contents data from the personal computer 103 next. And if SD card 104 in which desired contents data was incorporated is inserted in the general-purpose playback apparatus 105 the general-purpose playback apparatus 105 can reproduce desired contents by things.

[0008] However the duplicate more than a predetermined number is impossible for desired contents data by check-out of the personal computer 103 and the function of the system. The contents of the above-mentioned request Therefore a portable player a mini component When it is going to reproduce with two or more general-purpose playback apparatus 105 such as a car stereo there is inconvenience that SD card 104 in which contents data is recorded must be carried and SD card 104 must be set to the general-purpose playback apparatus 105 each time. In the above-mentioned method as for performing two or more reproduction even if it is less than a predetermined number since SD card 104 is comparatively expensive expense starts so much and there is a fault of being hard to spread through a user.

[0009] Thus in the above copyright management system it was hospitable to a contents distribution contractor's protection and there was the side in which the

user's user-friendliness had fallen victim.

[0010]How to use MD107 which is general-purpose media is shown in drawing 14 instead of using SD card 104. In the system shown in drawing 14a different point from the system shown in drawing 13 is a point of MD107 passing ID appendix sound apparatus 106 and being checked in and checked out by the personal computer 103. Namely in order to incorporate desired contents data into MD107. After checking that ID with which the personal computer 103 attests ID appendix sound apparatus 106 and ID appendix sound apparatus 106 is attested beforehand is given desired contents data is checked out by MD107 via ID appendix sound apparatus 106 from the personal computer 103.

[0011]Since cheap MD107 can be used according to such a system compared with a case where performing two or more reproductions reproduces using SD card 104 expense is cheap and ends. However for every transmission and reception of data since procedures such as attestation and cipher processing was required a highly efficient processing circuit was needed at check-in of ID appendix sound apparatus 106 to the personal computer 103 and check-out for ID appendix sound apparatus 106. Load of attestation and cipher processing is large and it is not easy to use a user.

[0012]The purpose of this invention aims at providing a user-friendly copyright protection system for a user a copyright protection method its host device its program and a medium that supported the program in consideration of above-mentioned SUBJECT.

[0013]

[Means for solving problem]The 1st this invention for solving an aforementioned problem While enciphering predetermined contents with a predetermined encryption method according to the number of playback equipment (5) to which reproduction was permitted It is a host device which sends decoding information (7) for choosing specific playback equipment (5) and decrypting said enciphered contents (6) to said specific selected playback equipment (5).

[0014]The 2nd this invention is the host device according to claim 1 further provided with a selection indication means for directing said selection.

[0015]The 3rd this invention is a host device of the 1st this invention with which said encryption uses host ID peculiar to said host device and apparatus ID and said host ID of said specific playback equipment (5) are contained in said decoding information (7).

[0016]The 4th this invention is a host device of the 1st this invention which said predetermined contents and information on said number (38) are enciphered from a distributing server (1) and is distributed.

[0017]Host ID which contents (6) as which the 5th this invention was enciphered by a host device have Apparatus ID which host ID contained in said decoding information (7) is in agreement and is contained in said decoding information (7) On condition that peculiar apparatus ID is in agreement are said enciphered contents (6) playback equipment to reproduce and said host device While enciphering predetermined contents

using peculiar host ID. Specific playback equipment (5) is chosen according to the number of playback equipment (5) to which reproduction was permitted. It is playback equipment which sends decoding information (7) in which apparatus ID and said host ID of said specific playback equipment (5) for decrypting said enciphered contents (6) are contained to said specific selected playback equipment (5).

[0018] The 6th this invention is playback equipment of the 5th this invention by which said playback equipment (5) is not connected to the Internet.

[0019] A distributing server (1) with which the 7th this invention distributes predetermined contents. Have a host device (3) which enciphers predetermined contents with a predetermined encryption method and playback equipment (5) which reproduces said enciphered contents and said host device (3). Said specific playback equipment (5) is chosen according to the number of playback equipment (5) to which reproduction was permitted. Sending decoding information (7) for decrypting said enciphered contents (6) to said specific selected playback equipment (5). Said playback equipment (5) is a copyright management system which reproduces said enciphered contents (6) using said sent decoding information (7).

[0020] A distributing server (1) with which the 8th this invention distributes predetermined contents. A host device (3) which enciphers said predetermined contents (1) with a predetermined encryption method. Are a copyright management system provided with playback equipment (5) which reproduces said enciphered contents the used copyright management method and said host device (3). Said specific playback equipment (5) is chosen according to the number of said playback equipment (5) to which reproduction was permitted. Sending decoding information for decrypting said enciphered contents (6) to said specific selected playback equipment (5). Said playback equipment (5) is the copyright management method which reproduces said enciphered contents (6) using said sent decoding information (7).

[0021] The 9th this invention is a program for operating the host device (3) which enciphers the predetermined contents of the copyright management system of the 7th this invention with a predetermined encryption method and the playback equipment (5) which reproduces said enciphered contents (6) as a computer.

[0022] The 10th this invention is the recording medium which made the program of the 9th this invention support and is an available recording medium by computer.

[0023]

[Mode for carrying out the invention] Hereafter it explains referring to Drawings for an embodiment of the invention.

[0024] Drawing 1 is a figure showing the outline of the composition of the copyright management system of this invention. In drawing 1 1 is an electronic music distribution (EMD) server and 2 an Internet line and 3 The personal computer of the users who have predetermined host ID which is an example of the host device of this invention and 4 are playback apparatus CD-R and whose 5 are examples of the playback equipment of this invention by which it is not connected to Internet line 2

and which has individual predetermined apparatus ID. In drawing 1 the apparatus A the apparatus B and the apparatus C are shown as the playback apparatus 5 reproduction is permitted to the apparatus A and the apparatus C and the state where reproduction is not permitted is shown in the apparatus B. Each playback apparatus 5 is composition connectable with the personal computer 3 with a telecommunication cable.

[0025] Next the outline of operation of such a copyright management system is explained. First a user downloads contents data via Internet line 2 with users' personal computer 3 from EMD server 1. The personal computer 3 enciphers the downloaded contents data by a predetermined method and copies to CD-R4. At this time it may be copied to two or more CD-R4 with the personal computer 3 and CD-R4 of one sheet created may be copied to two or more CD-R4. A user inserts CD-R4 in the apparatus A or the apparatus C which is the playback apparatus 5 decided beforehand. The apparatus A or the apparatus C permitted reproduction can reproduce desired contents. At this time even if a user inserts CD-R4 in the apparatus B by which reproduction is not permitted desired contents are unreproducible. Thus the contents data copied to CD-R4 whose points of the copyright management system of this invention are general-purpose media is renewable only with the playback apparatus 5 in which it was enciphered by the original system of the personal computer 3 and reproduction was permitted beforehand.

[0026] Drawing 2 shows the outline of operation that contents data is not reproduced only to the predetermined playback apparatus 5. The personal computer 3 has ID001 as host ID. The playback apparatus 5 has ID00A as apparatus ID. And the personal computer 3 enciphers desired contents data by a predetermined method to CD-R4 and gives ENC001 which is encryption ID using host ID. That is the enciphered contents 6 which have ENC001 are recorded on CD-R4. The personal computer 3 generates the decode key 7 which is an example of the decoding information on this invention in one side. This decode key 7 has ID00A which is DEC001 which is ID for decoding created using host ID for decoding the enciphered contents and apparatus ID of the playback apparatus 5. And the decode key 7 is transmitted to the playback apparatus 5 from the personal computer 3.

[0027] A user inserts CD-R4 in which the enciphered contents were accommodated in the playback apparatus 5. The playback apparatus 5 verifies whether ENC001 contained in the enciphered contents and DEC001 which are contained in the decode key correspond. It is verified whether apparatus ID00A contained in the decode key 7 and apparatus ID00A of playback apparatus 5 which is apparatus ID peculiar to the playback apparatus 5 correspond. In verification of above both when correspondence and coincidence are obtained the playback apparatus 5 can reproduce desired contents by decrypting the enciphered contents which are contained in CD-R4.

[0028] Drawing 3 is a block diagram showing an example of the composition of the personal computer 3. 22 is a means of communication for receiving distribution of the

contents enciphered by the general-purpose encryption method in EMD server 1 via Internet line 2 and 23. It is a contents acquiring means for acquiring the contents enciphered from said means of communication 22. 8 is a decoding means for decoding the enciphered contents which came to hand with a general-purpose decoding method. 9 is a contents encryption means which enciphers the decrypted contents using ID for encryption and 10 is a recording device for recording the enciphered contents on CD-R4.

[0029] 14 is the self-ID holding mechanism holding host ID and 15 is a self-ID acquiring means for acquiring host ID from the self-ID holding mechanism. 14, 16 is ID for codes from host ID and ID for decoding which were acquired. ID creating means for ID decoding for codes for generating and 17 are a decode key creating means for generating a decode key using ID generated by the ID creating means. 16 for ID decoding for codes and ID generated by the apparatus ID acquiring means 20 and 18. It is a decode key issuing means for publishing the decode key generated by the decode key creating means 17 to the playback apparatus 5.

[0030] 11 is a key acquiring means for the number information 38 (after-mentioned) to come to hand from 1 via the means of communication 22. 13 is a lock management information control means and 12 is a lock management information database.

[0031] 19 is a means of communication for communicating with the playback apparatus 5. 20 is an apparatus ID acquiring means for apparatus ID to come to hand from the playback apparatus 5 via the means of communication 19 and 21 is a decode key deleting means for deleting the decode key published by the playback apparatus 5.

[0032] Above-mentioned ID creating means 16 for ID decoding for codes, decode key creating means 17, decode key issuing means 18 and decode key deleting means 21 correspond as an example of the selection indication means of this invention.

[0033] Drawing 4 is a block diagram showing an example of composition of the playback apparatus 5. In drawing 4, 24 is a media drive for driving CD-R4 and 25 is ID extraction means for codes for extracting ID for codes from contents recorded on CD-R4 set to the media drive 24. 26 is a means of communication for communicating with the personal computer 3 and 27 is the decode key holding mechanism for holding the decode key 7 published with the personal computer 3. 28 is a decode key acquisition means for acquiring the decode key 7 from the means of communication 26 or the decode key holding mechanism 27. 37 is ID extraction means for decoding for extracting ID for decoding from the decode key acquisition means 28. 30 is an apparatus ID extraction means for extracting apparatus ID from the decode key 7 acquired in the decode key acquisition means 28. 31 is the apparatus ID holding mechanism for holding apparatus ID peculiar to each playback apparatus 5 and 33 is an apparatus ID comparison means for comparing apparatus ID acquired in apparatus ID acquiring means 32 with apparatus ID extracted in the apparatus ID extraction means 30.

[0034] From the comparison result in a code, the ID comparison means 29 for

decoding and the apparatus ID comparison means 3334. It is a reproduction propriety judging means which judges whether it is possible to reproduce desired contents in the playback apparatus 535 is a decode processing means for decoding the enciphered contents data which is supplied from the media drive 24 based on the decided result in the reproduction propriety judging means 34 and 36 is an output means for carrying out the reproducing output of the contents by which decoding processing was carried out in the decode processing means 35.

[0035] Next the details of operation of the copyright management system of this invention of the above composition are explained referring to drawing 5 and drawing 6. Drawing 5 is a figure explaining the operation in the copyright management whole system. Drawing 6 is a flow chart of the whole copyright management system of this invention.

[0036] First a user demands distribution of the number information 38 via Internet line 2. That is admission in service is required of the EMD server 1 side (Step 101). Information on the number of a reproducing permission of the playback apparatus 5 for which a user wishes is included in this demand. In EMD server 1 when accepting a user's subscription the number information 38 is distributed via Internet line 2 (Step 102). In this number information 38 the number of a reproducing permission of an individual user who wishes to register as a club member is contained.

[0037] And when a user wishes distribution of contents the personal computer 3 transmits a distribution request of desired contents to EMD server 1 via Internet line 2 (Step 103). EMD server 1 will transmit contents data and the number information 38 which enciphered contents for which a user asks with a general-purpose encryption method to the personal computer 3 via Internet line 2 if a contents distribution demand is received (Step 104). The personal computer 3 will decode contents data and the number information 38 which were enciphered by a general-purpose decoding method if contents data and the number information 38 which were enciphered are received.

[0038] If CD-R4 is set to the personal computer 3 by user and predetermined operation is carried out the personal computer 3 will encipher using host ID and will record decrypted contents on CD-R4 (Step 105).

[0039] And when reproducing CD-R4 on which contents as which a user was enciphered were recorded in the playback apparatus 5 the playback apparatus 5 performs issue requesting of the decode key 7 first (Step 106). When the playback apparatus 5 has the decode key 7 and when applying a trigger from the personal computer 3 to the playback apparatus 5 this step 106 becomes unnecessary.

[0040] The personal computer 3 will advance a Request to Send of apparatus ID of the playback apparatus 5 to the playback apparatus 5 if issue requesting of the decode key 7 is received from the playback apparatus 5 (Step 107). If the playback apparatus 5 receives a Request to Send of apparatus ID the playback apparatus 5 will send apparatus ID peculiar to the playback apparatus 5 to the personal computer 3 (Step

108). And the personal computer 3 generates the decode key 7 from ID00A which is apparatus ID peculiar to DEC001 and the playback apparatus 5 which are ID for decoding generated from host ID peculiar to the personal computer 3. And the personal computer 3 sends the generated decode key 7 to the playback apparatus 5 (Step 109).

[0041]When a user is going to reproduce desired contents in the playback apparatus 5 the playback apparatus 5 advances a reproduction request of enciphered content to CD-R4 (Step 110). In the playback apparatus 5 ENC001 recorded on the contents 6 as which CD-R4 was enciphered is compared with DEC001 which are contained in the decode key 7 transmitted from the personal computer 3 and it verifies that it is that to which both correspond. That is it verifies that 001 which is host ID is in agreement in both. It is verified whether ID00A which is apparatus ID contained in the decode key 7 and ID00A of playback apparatus 5 which is apparatus ID peculiar to the playback apparatus 5 correspond. And if it is checked that conditions of above both are fulfilled the playback apparatus 5 will decrypt the enciphered contents 6 and will reproduce desired contents (Step 111).

[0042]In drawing 5 the portion by which the center section was surrounded shows the processing in the dedicated software for exchanging the data of EMD server 1 and the personal computer 3. The portion surrounded in the lower right in the figure direction shows the processing in the dedicated software for exchanging the data between the playback apparatus 5 and the personal computer 3. In such dedicated software since processing is performed protecting the data of a key etc. so that it may not be accessed from the outside the information transmitted and received is not revealed outside.

[0043]Drawing 7 is the flow chart which illustrated operation of the personal computer 3 in the above-mentioned copyright management system. Operation of the personal computer 3 is explained below referring to drawing 3 and drawing 7.

[0044]Drawing 7 (a) is a flow when copying desired contents data to CD-R4. A user starts operation of the personal computer 3 first (Step 210). And the personal computer 3 demands determination of whether to newly purchase the number information 38 from a user (Step 211). When judging that the number information 38 is purchased the personal computer 3 carries out purchase processing of the number information 38 (Step 212) and the lock management information control means 13 of the personal computer 3 registers lock management information into the lock management information database 12 (Step 213). The number information 38 already exists and when it is not newly necessary to purchase it progresses to the following step.

[0045]In Step 213 if lock management information is registered the personal computer 3 will demand determination of whether to purchase contents next from a user (Step 214). If it is determined that contents are purchased the contents acquiring means 23 of the personal computer 3 will perform purchase processing of contents via the

means of communication 22 (Step 215). Processing is ended when it is determined that contents are not purchased (Step 218). If content purchase processing is completed in Step 215 the decoding means 8 will decrypt contents enciphered with a general-purpose decoding method. And the contents encryption means 9 enciphers contents using ID for codes generated by the ID creating means 16 for ID decoding for codes (Step 216). The recording device 10 copies enciphered contents to CD-R4 (Step 217) and ends processing (Step 218).

[0046] Drawing 7 (b) is a flow in case the personal computer 3 generates a decode key to the playback apparatus 5 by which the reproducing permission was carried out. First the personal computer 3 makes the issue processing of a decode key start (Step 220). And the personal computer 3 issues the directions which acquire the decode key 7 from the playback apparatus 5 (Step 221). Next the personal computer 3 verifies whether the playback apparatus 5 has the decode key 7 (Step 222). When the playback apparatus 5 has already had the decode key 7 it is judged whether the decode key 7 is deleted (Step 223). Processing is ended when not deleting the decode key 7 (Step 230). When the playback apparatus 5 does not have the decode key 7 the personal computer 3 progresses to the following step. In the following step the lock management information control means 13 obtains lock management information from the lock management information database 12 (Step 225) and passes it to the decode key creating means 17.

[0047] On the other hand the apparatus ID acquiring means 20 acquires apparatus ID from the playback apparatus 5 via the means of communication 19 (Step 226) and it is judged whether issue of the decode key 7 is appropriate for the decode key creating means 17 (Step 227). Processing is ended when issue of the decode key 7 is not appropriate (Step 230). When issue of the decode key 7 is appropriate the decode key creating means 17 generates the decode key 7 from ID for decoding obtained from the ID creating means 16 for ID decoding for codes and apparatus ID acquired from the playback apparatus 5 (Step 228). And the decode key issuing means 18 transmits the decode key 7 to the playback apparatus 5 and ends processing (Step 229) (Step 230).

[0048] Drawing 7 (c) shows an example of lock management information stored in the lock management information database 12. A situation where the decode key 7 is published to one set of the playback apparatus 5 in which a user has got three sets of the number of a reproducing permission from EMD server 1 and this lock management information has ID of ID00A is shown. An acquisition day of a key and the date of issue of the decode key 7 are recorded on this lock management information.

[0049] Drawing 8 shows a process flow by the side of the playback apparatus 5. Step 341 in drawing 8 (a) – Step 344 are equivalent to Step 106 in drawing 6 – Step 109. An operation flow of the playback apparatus 5 is explained below referring to drawing 8 and drawing 4.

[0050] In drawing 8 (a) the playback apparatus 5 starts processing of a decode key

demand first (Step 340). The means of communication 26 transmits the issue requesting of the decode key 7 to the personal computer 3 side (Step 341). If transmission of apparatus ID of the playback apparatus 5 is required from the personal computer 3 side the decode key acquisition means 28 will transmit apparatus ID currently held at the apparatus ID holding mechanism 31 to the personal computer 3 side via the means of communication 26 (Step 342). If a decode key is published from the personal computer 3 the means of communication 26 receives the published decode key 7 (Step 343) and the decode key acquisition means 28 will register the acquired decode key 7 into the decode key holding mechanism 27 (Step 344) and it will end processing (Step 345).

[0051] Drawing 8 (b) is an operation flow figure at the time of reproducing contents in the playback apparatus 5.

[0052] First the playback apparatus 5 starts contents playback processing by a user's operation (Step 350). The decode key acquisition means 28 checks whether the decode key holding mechanism 27 possesses the decode key 7 (Step 351). When the decode key 7 does not exist in the decode key holding mechanism 27 it progresses to the step of whether to acquire the decode key 7 (Step 352). In this step 352 when not acquiring the decode key 7 processing is ended (Step 361) and when acquiring the decode key 7 it progresses to the decode key demand flow shown in drawing 8 (a) (Step 353). When the decode key 7 exists in the decode key holding mechanism 27 apparatus ID and apparatus ID of the playback apparatus 5 which are contained in the decode key 7 are compared (Step 354). Namely the apparatus ID extraction means 30 extracts apparatus ID from the decode key 7 which exists in the decode key acquisition means 28 and passes it to the apparatus ID comparison means 33. Apparatus ID acquiring means 32 acquires peculiar apparatus ID which exists in the apparatus ID holding mechanism 31 and passes it to the apparatus ID comparison means 33. And it is compared whether apparatus ID passed from the apparatus ID extraction means 30 and apparatus ID of the apparatus ID comparison means 33 passed from apparatus ID acquiring means 32 correspond (Step 355). Processing is ended when both apparatus ID is not in agreement (Step 361).

[0053] When both apparatus ID is in agreement ID extraction means 25 for codes acquires ID for codes contained in contents from the media drive 24 (Step 356) and passes it to a code and the ID comparison means 29 for decoding. On the other hand ID extraction means 37 for decoding extracts ID for decoding from the decode key 7 which exists in the decode key acquisition means 28 and passes it to a code and the ID comparison means 29 for decoding. And a code and the ID comparison means 29 for decoding compare ID for codes acquired from enciphered contents with ID for decoding contained in the decode key 7 (Step 357). That is a code and the ID comparison means 29 for decoding compare ID for codes with ID for decoding and both verify whether it is a thing corresponding to the same host ID (Step 358).

[0054] When above-mentioned ID for codes and ID for decoding do not correspond the

reproduction propriety judging means 34 carries out a judgment of being unreplicable and ends processing (Step 361). When it is that to which both ID correspond, take out the reproduction propriety judging means 34 and a renewable judgment the decode processing means 35. Decrypting the enciphered contents 6 using the decode key 7 (Step 359) by outputting decrypted contents, the output means 36 reproduces contents for which a user asks (Step 360) and ends processing (Step 361).

[0055] Drawing 9 is a mimetic diagram showing the whole copyright management system of this invention in case there is two or more sets of the playback apparatus 5 by which the reproducing permission was carried out. In the example shown in drawing 9, the case where two sets, the apparatus A which is a portable CD player among the playback apparatus 5 and the apparatus B which is mini components, have obtained the reproducing permission is shown. In such a case, as ID for decoding, the personal computer 3 generates the decode key 7 which has ID00A as DEC001 and apparatus ID to the apparatus A and generates to it the decode key 7 which has 00B as DEC001 and apparatus ID as ID for decoding at the apparatus B. And these decode keys 7 are transmitted to the apparatus A and the apparatus B respectively.

[0056] Herein order to reproduce the enciphered contents 6 by the apparatus A and in order to reproduce by the apparatus B, two CD-R4 are copied in the personal computer 3. At this time, the enciphered same contents 6 are recorded on each CD-R4. That is, ENC001 is stored in the enciphered contents 6 as a key for codes with the enciphered same contents data.

[0057] The apparatus A and the apparatus B decrypt the contents 6 enciphered with the decode key 7 which each has and reproduce desired contents.

[0058] Drawing 10 illustrates a variation from which copyright is protected by a copyright management system of this invention by composition to the above and operation.

[0059] In drawing 10a, a case where another different personal computer 43 exists is shown in the personal computer 3 as a host device. Three sets, the apparatus A, the apparatus B and the apparatus C exist as the playback apparatus 5 among these, the apparatus A shows the state that the decode key 7 was published with the personal computer 3 and of being the playback apparatus 5.

[0060] On the above conditions, a case where illegal acquisition of the CD-R on which contents were first recorded with the personal computer 43 which is a third party's personal computer is carried out is considered. In this case, the personal computer 43 enciphers contents to CD-R4 inserted in the personal computer 43 using ID002 which is host ID of the personal computer 43 and ENC002 is contained in the enciphered contents 46 as an encryption key. If a user is going to reproduce desired contents using the apparatus A, when it has the contents 46 as which CD-R4 was enciphered (i.e. when ENC002 exists in the enciphered contents 46), the apparatus A. As mentioned above, DEC001 which is ID for decoding contained in the decode key 7 which the apparatus A has is compared with ENC002 which are contained in the enciphered

contents 46 and both check not originating in the same host ID. Therefore the apparatus A cannot reproduce contents obtained by CD-R recorded with the personal computer 43 in this way coming to hand unjustly.

[0061] Next, supposing the decode key 7 is not published by the apparatus B, the apparatus B can reproduce neither the contents copied with the personal computer 3 nor the contents copied with the personal computer 43 though natural.

[0062] Next, the apparatus C assumes that it does not have the regular decode key 7 but has what copied the decode key 7 of the apparatus A unjustly. In that case, since the peculiar apparatus ID which the apparatus C has is ID00C and the apparatus ID which exists in the decode key 7 copied illegally by one side is ID00A, it is judged that the apparatus ID of apparatus C of both does not correspond. Therefore, in the apparatus C which copied the decode key 7 illegally, desired contents are unreproducible. Of course, the contents copied illegally with the personal computer 43 are also unreproducible.

[0063] Drawing 11 is the figure which made the list the range from which copyright is protected as mentioned above at a case. That is, the playback apparatus 5 is an apparatus which has the regular decode key 7 by which the reproducing permission was carried out and only when CD-R4 is copied with a user's regular personal computer 3, the contents for which a user asks can be reproduced. However, such contents cannot be reproduced when the playback apparatus 5 is an apparatus which does not have the decode key 7 and when the playback apparatus 5 is an apparatus which has copied the decode key 7 illegally.

[0064] Drawing 12 is a figure showing a flow when changing the playback apparatus 5 by which the reproducing permission was carried out without changing the number of a reproducing permission of the playback apparatus 5.

[0065] For example, the user shall have three sets of the playback apparatus 5, the apparatus A, the apparatus B, and the apparatus C. Among these, the reproducing permission shall be made by two sets, the apparatus A and the apparatus B. And the number of a reproducing permission of two sets makes an example the case where reproducing permission apparatus is changed into the apparatus B and the apparatus C from the apparatus A and the apparatus B without changing and a user explains operation of the copyright management system of this embodiment in that case below.

[0066] In drawing 12, Step 401 is equivalent to Step 101 – Step 104 which are shown in drawing 6. Step 402 corresponds to 105 shown in drawing 6 and Step 403 – Step 406 are equivalent to Step 106 – Step 109 which are shown in drawing 6. The operation corresponding to Step 403 – Step 406 in Step 407 – Step 410 is made between the personal computer 3 and the apparatus B. In the apparatus A and the apparatus B, operation can reproduce so far the contents for which a user asks in the state of ** practice ***** (Step 411, Step 412). However, the apparatus C which does not have the decode key 7 cannot reproduce contents (Step 413).

[0067] Next, the personal computer 3 advances a Request to Send so that the decode

key 7 which the apparatus A has may be transmitted to the apparatus A (Step 414). And if the apparatus A receives the Request to Send of the decode key 7 from the personal computer 3 the decode key 7 which the apparatus A has will be transmitted to the personal computer 3 and the decode key 7 will be deleted from the apparatus A (Step 415). The decode key 7 of the apparatus A received also in the personal computer 3 is deleted by the decode key deleting means 21 (Step 224 (refer to drawing 7 (b)))).

[0068] And between the apparatus C and the personal computer 3 the decode key 7 is transmitted to the apparatus C in Step 416 – Step 419 by the same processing as Step 403 – Step 406. As a result by the apparatus A desired contents cannot be reproduced (Step 420) but desired contents can be reproduced in the apparatus B and the apparatus C (Steps 421 and 422).

[0069] As mentioned above according to the copyright management system of carrying of this embodiment since two or more sheet copy is possible to general-purpose CD-R4 desired contents When reproducing with two or more playback apparatus 5 a portable player a minicomponent a car stereo etc. can be set to each playback apparatus 5 and do not need to apply the time and effort which carries CD-R4 one by one.

[0070] According to the copyright management system of this embodiment by restricting the number of the playback apparatus 5 reproduced instead of what restricts a duplicate of CD-R4 although protection of copyright is aimed at a user's convenience can be raised.

[0071] Since EMD server 1 does not need to perform license management of the individual playback apparatus 5 and should manage only the number of licence of the playback apparatus 5 it can be managed with an easy system configuration also for the EMD server 1 side.

[0072] Since the decode key 7 for decoding desired contents is published in users' personal computer 3 the user does not need to ask the EMD server 1 side one by one and can enjoy desired contents by easy processing.

[0073] Although explanation to the above is related with a copyright management system of this invention a copyright management method using a system of the above-mentioned composition is also the range of this invention.

[0074] In explanation to the above although distribution of the number information 38 from EMD server 1 in Step 101 to the personal computer 3 presupposed that it is made via Internet line 2 it may be transmitted or sent for example by other methods such as mail.

[0075] Although it presupposed that the personal computer 3 and the playback apparatus 5 are connected with a telecommunication cable and an exchange of the decode key 7 etc. are made in explanation to the above the personal computer 3 and the playback apparatus 5 may be compositionally connected not by a cable but by radio. It may be the composition that an exchange of the decode key 7 etc. are made using

physical media such as CD-R. In that case the exchange of the decode key 7 grade between the personal computer 3 and the playback apparatus 5 serves as operation instead of transmission or reception sent or received. The effect same also in such a case as the above can be acquired.

[0076] Although they presupposed that it is CD-Reven if the media on which the enciphered contents are recorded in explanation to the above are other media naturally they are good.

[0077] Although the personal computer 3 presupposed that the decode key 7 is published to the playback apparatus 5 within the number by which the reproducing permission was carried out in explanation to the above there may be a function to restrict issue of the decode key 7 to still more specific apparatus. As such an example it may be the composition of publishing the decode key 7 only to the playback apparatus 5 corresponding to high-quality sound for example.

[0078] Not only music data but the information on still picture information a video data alphabetic data and others is included in the contents in explanation to the above. That is the distributing server of this invention may be a server which is not limited to EMD server 1 but can distribute above various contents.

[0079] Although it presupposed that the host devices of this invention are the personal computers 3 and 43 in explanation to the above as long as the host device of this invention can achieve the above-mentioned function they may be apparatus other than a personal computer. Although a cellular phone a personal digital assistant etc. are mentioned as such an example it is not limited to these.

[0080] Although the playback apparatus 5 explained the example which is one set or three sets by explanation to the above if the playback apparatus 5 is less than the number of a reproducing permission it cannot be overemphasized that they may be how many sets. What is necessary is just to notify change of the number of a reproducing permission to the distributing server side in Step 101 shown in drawing 6 to change the number of a reproducing permission.

[0081] The program of this invention is a program for performing the function of all or a part of means (or equipment an element etc.) of the copyright management systems of this invention mentioned above by computer and is a program which collaborates with a computer and operates.

[0082] All or a part of means (.) of the copyright management systems of this invention which the recording medium of this invention mentioned above Or it is the recording medium which supported the program for performing the function of all or the parts of equipment an element etc. by computer and said program which reading was possible and was read by computer is a recording medium which cooperates with said computer and performs said function.

[0083] The above "some means (or equipment an element etc.)" of this invention means one or some means of two or more of those means and the above "some steps (or a process operation an operation etc.)" of this invention means one or some steps of two

or more of those steps.

[0084]The above "function of MEANS (or equipmentan elementetc.)" of this invention means the function of all or a part of said meansand the above "operations (or a processoperationan operationetc.) of a step" of this invention means operation of all or a part of said steps.

[0085]One usage pattern of the program of this invention may be a mode which is recorded on the recording medium which can be read by computercollaborates with a computerand operates.

[0086]One usage pattern of the program of this invention may be a mode which transmits the inside of a transmission mediumis read by computercollaborates with a computerand operates.

[0087]As a data structure of this inventionthe kind of a databasaea data formata data tablea data listand dataetc. are included.

[0088]As a recording mediumROM etc. are contained and transmission mediasuch as the Internetlightan electric wavea sound waveetc. are contained as a transmission medium.

[0089]The computer of this invention mentioned above may contain not only hardware with pure and simple CPU etc. but firmwareand OS and also peripheral equipment.

[0090]As explained aboveit may realize by software and composition of this invention may be realized in hardware.

[0091]

[Effect of the Invention]According to this inventionthe user-friendly copyright protection system for a userthe copyright protection methodits host deviceits programand the recording medium that supported the program can be provided.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]Drawing 1 is a figure showing the outline of the copyright management system of an embodiment of the invention.

[Drawing 2]Drawing 2 is a figure showing the outline of operation of the copyright management system of an embodiment of the invention.

[Drawing 3]Drawing 3 is a block diagram showing the composition of the personal computer which constitutes the copyright management system of an embodiment of the invention.

[Drawing 4]Drawing 4 is a block diagram showing the composition of the playback apparatus which constitutes the copyright management system of an embodiment of the invention.

[Drawing 5]Drawing 5 is a schematic view showing operation of the whole copyright management system of an embodiment of the invention.

[Drawing 6] Drawing 6 is a flow chart showing operation of the whole copyright management system of an embodiment of the invention.

[Drawing 7] Drawing 7 is a flow chart showing operation of the personal computer which constitutes the copyright management system of an embodiment of the invention.

[Drawing 8] Drawing 8 is a flow chart showing operation of the playback apparatus which constitutes the copyright management system of an embodiment of the invention.

[Drawing 9] Drawing 9 is a schematic view showing operation of the whole copyright management system of an embodiment of the invention.

[Drawing 10] Drawing 10 is a figure showing the variation of the copyright protected by the copyright management system of an embodiment of the invention.

[Drawing 11] Drawing 11 is a figure showing the variation of the copyright protected by the copyright management system of an embodiment of the invention.

[Drawing 12] Drawing 12 is a flow chart showing the operation at the time of making a number change of a reproducing permission of the playback apparatus which constitutes the copyright management system of an embodiment of the invention.

[Drawing 13] Drawing 13 is a schematic view of the copyright management system of conventional technology.

[Drawing 14] Drawing 14 is a schematic view of the copyright management system of conventional technology.

[Explanations of letters or numerals]

1 EMD server

2 Internet line

3 and 43 A personal computer

4 CD-R

5 Playback apparatus

6 Enciphered contents

7 A decode key

8 A decoding means

9 A contents encryption means

10 A recording device

11 A key acquiring means

12 A lock management information database

13 A lock management information control means

14 Self-ID holding mechanism

15 A self-ID acquiring means

16 ID creating means for ID decoding for codes

17 A decode key creating means

18 A decode key issuing means

19, 22 and 26 A means of communication

- 20 An apparatus ID acquiring means
 - 21 A decode key deleting means
 - 23 A contents acquiring means
 - 24 A media drive
 - 25 ID extraction means for codes
 - 27 Decode key holding mechanism
 - 28 A decode key acquisition means
 - 29 An ID comparison means for cipher items
 - 30 An apparatus ID extraction means
 - 31 Apparatus ID holding mechanism
 - 32 An apparatus ID acquiring means
 - 33 An apparatus ID comparison means
 - 34 A reproduction propriety judging means
 - 35 Decode processing means 36 An output means
 - 37 ID extraction means for decoding
 - 38 A key
-

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-323351

(P2003-323351A)

(43) 公開日 平成15年11月14日 (2003. 11. 14)

(51) Int.Cl. ⁷	識別記号	F I	テ-マコ-ト* (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 F 5 B 0 1 7 3 2 0 E 5 D 0 4 4
G 1 1 B 20/10		G 1 1 B 20/10	H 5 D 1 1 0
20/12		20/12	5 J 1 0 4
27/00		27/00	D
審査請求 未請求 請求項の数10 O L (全 16 頁) 最終頁に続く			

(21) 出願番号 特願2003-50043 (P2003-50043)

(22) 出願日 平成15年2月26日 (2003. 2. 26)

(31) 優先権主張番号 特願2002-50963 (P2002-50963)

(32) 優先日 平成14年2月27日 (2002. 2. 27)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 宮本 晴敏

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 100092794

弁理士 松田 正道

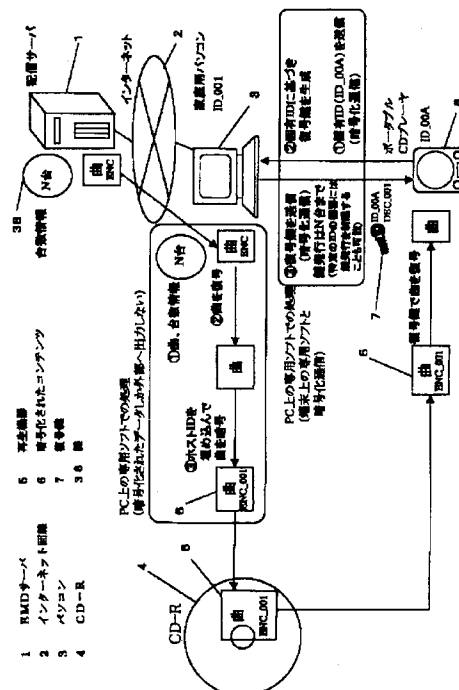
最終頁に続く

(54) 【発明の名称】 著作権管理システム、著作権管理方法、ホスト装置、プログラムおよび記録媒体

(57) 【要約】

【課題】 ユーザにとって使い勝手がよい著作権保護システム、著作権保護方法、そのホスト装置、そのプログラム、そのプログラムを担持した記録媒体を提供すること。

【解決手段】 所定のコンテンツを所定の暗号化方法で暗号化するとともに、あらかじめ再生を許可された再生装置5の台数に応じて、特定の再生装置5を選択し、前記選択された特定の再生装置5へ、前記暗号化されたコンテンツ6を復号化するための復号鍵等の復号化情報を送るホスト装置。



【特許請求の範囲】

【請求項1】 所定のコンテンツを所定の暗号化方法で暗号化するとともに、再生を許可された再生装置の台数に応じて、特定の再生装置を選択し、前記選択された特定の再生装置へ、前記暗号化されたコンテンツを復号化するための復号化情報を送るホスト装置。

【請求項2】 前記選択を指示するための選択指示手段をさらに備える、請求項1に記載のホスト装置。

【請求項3】 前記暗号化は、前記ホスト装置に固有のホストIDを利用したものであり、前記復号化情報には、前記特定の再生装置の機器IDと、前記ホストIDが含まれている、請求項1に記載のホスト装置。

【請求項4】 前記所定のコンテンツおよび前記台数の情報は、配信サーバから暗号化されて配信されたものである、請求項1に記載のホスト装置。

【請求項5】 ホスト装置により暗号化されたコンテンツが有するホストIDと、前記復号化情報に含まれているホストIDとが一致し、かつ、前記復号化情報に含まれる機器IDと、固有の機器IDとが一致していることを条件として、前記暗号化されたコンテンツを再生する再生装置であって、

前記ホスト装置は、所定のコンテンツを固有のホストIDを利用して暗号化するとともに、再生を許可された再生装置の台数に応じて、特定の再生装置を選択し、前記選択された特定の再生装置へ、前記暗号化されたコンテンツを復号化するための、前記特定の再生装置の機器IDおよび前記ホストIDが含まれている復号化情報を送る、再生装置。

【請求項6】 前記再生装置は、インターネットに接続されていない、請求項5に記載の再生装置。

【請求項7】 所定のコンテンツを配信する配信サーバと、所定のコンテンツを所定の暗号化方法で暗号化するホスト装置と、前記暗号化されたコンテンツを再生する再生装置と、を備え、

前記ホスト装置は、再生を許可された再生装置の台数に応じて、特定の前記再生装置を選択し、前記選択された特定の再生装置へ、前記暗号化されたコンテンツを復号化するための復号化情報を送り、前記再生装置は、前記送られた復号化情報を利用して、前記暗号化されたコンテンツを再生する著作権管理システム。

【請求項8】 所定のコンテンツを配信する配信サーバと、前記所定のコンテンツを所定の暗号化方法で暗号化するホスト装置と、前記暗号化されたコンテンツを再生する再生装置と、を備える著作権管理システムを利用した著作権管理方法であって、

あって、

前記ホスト装置は、再生を許可された前記再生装置の台数に応じて、特定の前記再生装置を選択し、前記選択された特定の再生装置へ、前記暗号化されたコンテンツを復号化するための復号化情報を送り、前記再生装置は、前記送られた復号化情報を利用して、前記暗号化されたコンテンツを再生する著作権管理方法。

【請求項9】 請求項7に記載の著作権管理システムの、所定のコンテンツを所定の暗号化方法で暗号化するホスト装置と、前記暗号化されたコンテンツを再生する再生装置と、をコンピュータとして機能させるためのプログラム。

【請求項10】 請求項9に記載のプログラムを担持させた記録媒体であって、コンピュータで利用可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンテンツの著作権のライセンス管理を行う著作権管理システム、著作権管理方法、そのホスト装置、そのプログラム、およびそのプログラムの記録媒体に関する。

【0002】

【従来の技術】近年、CD-DAのみならず、mp3 (mpeg audio layer 3) のような元の音源から複製された音楽形式がユーザーに広く利用されている。しかし、mp3などには著作権管理の方法が確立していないため著作権者にとって大きな問題となっており、これを解決しようとする手段が提案されている。また音楽だけでなく、映像や画像といったデジタルコンテンツについても著作権管理の方法が検討されている。例えば、パソコン上で用いられるWMA (Windows (登録商標) Media Audio) という音楽圧縮方式の著作権管理においてはDRM (Digital Right Management) と呼ばれる方式が採用されている。これは、暗号化された音楽の復号化には、暗号化した装置の固有IDが必要となる方式であり、暗号化装置と再生装置を同一の装置に限定することで違法コピーの蔓延を防ぐことができる。また、携帯電話等の小型端末をターゲットとした情報配信システムにおいても、配信情報の著作権を保護する方式が提案されている (例えば、特許文献1参照)。配信サーバから配信された情報と配信先の携帯電話の固有IDとを、サーバ上の管理データベースに登録しておき、登録された携帯電話でしか情報を再生できない仕組みとなっている。

【0003】

【特許文献1】特開2001-78266号公報

【0004】

【発明が解決しようとする課題】しかし、それぞれの装置がネットワーク上のサーバーにアクセスできることが前提となるため、ネットワーク接続を前提としない再生装置などで実現できるものではない。

【0005】また、直接ネットワークにアクセスできない再生装置で著作権のライセンス管理を行う方法として、図13に示す方法がある。図13において、101は、電子音楽配信（EMD）サーバであり、102はインターネット回線、103はユーザ側のパソコン、104は固有IDをもつメディア、例えばSDカード（Secure Digitalカード）、105は、インターネット回線に接続されていない汎用再生機器105である。

【0006】ここで、パソコン103とSDカード104との間には、チェックイン、チェックアウト方式でデータが送受信される。データのチェックイン、チェックアウトとは、データのコピー回数を管理しながらパソコンと外部機器、メディアとの間でデータを送受信することをいう。チェックアウトとは、データをパソコンから外部機器、メディアに転送することをいう。この場合データにチェックアウト（コピー）の制限回数がある場合には、制限回数を超えるチェックアウトはできない。チェックインとは、パソコンから外部機器、メディアに転送されたデータを、それらの外部機器、メディアに残らないように転送元のパソコンに戻すことをいう。なお、この場合、チェックアウトされたデータは転送元のパソコンにしか戻すことができない。しかし、チェックインによりパソコンに戻されたデータは、再びチェックアウトすることができる。

【0007】この方法によれば、コンテンツをメディアであるSDカード104の固有IDと一緒に扱うことで、コンテンツのオリジナルと複製を区別して著作権管理を行う。具体的には、認証されたSDカード104にのみコンテンツのデータをチェックアウトすることにより、データの不正コピーを防止するものである。すなわち、ユーザは、EMDサーバ101からインターネット回線102を介してユーザ側のパソコン103でコンテンツデータをダウンロードする。SDカード104がパソコン103に挿入されることにより、パソコン103は、SDカード104があらかじめ認証されている所定のIDが付与されていることを確認する。パソコン103は次にパソコン103からコンテンツデータをチェックアウトする。そして、所望のコンテンツデータが取り込まれたSDカード104を汎用再生機器105に挿入するとことにより、汎用再生機器105は、所望のコンテンツを再生することができる。

【0008】しかし、パソコン103のチェックアウト、チェックインの機能により、所望のコンテンツデータは、所定数以上の複製が不可能である。従って、上記の所望のコンテンツを、ポータブルプレーヤ、ミニコン

ポ、カーステレオ等複数の汎用再生機器105で再生しようとする場合、コンテンツデータが記録されているSDカード104を持ち運びその都度SDカード104を汎用再生機器105にセットしなければならない、という不都合がある。また、上記の方法では、SDカード104が比較的高価であるため、所定数以内であっても複数の複製を行うことは、それだけ費用がかかってしまい、ユーザに普及しにくいという欠点がある。

【0009】このように、上記のような著作権管理システムでは、コンテンツ配信業者の保護に手厚く、ユーザの使い勝手が犠牲になっている側面があった。

【0010】SDカード104を使用する代わりに汎用メディアであるMD107を使用する方法を図14に示す。図14に示すシステムにおいて、図13に示すシステムと異なる点は、MD107は、ID付録音機器106を介してパソコン103にチェックイン、チェックアウトされる点である。すなわち、MD107に所望のコンテンツデータを取り込むためには、パソコン103は、ID付録音機器106を認証し、ID付録音機器106があらかじめ認証されているIDが付与されていることを確認した後、所望のコンテンツデータは、パソコン103からID付録音機器106を介してMD107にチェックアウトされる。

【0011】このようなシステムによれば、廉価なMD107を使用することができるので、複数の複製を行うことはSDカード104を使用して複製する場合に比べて費用は安く済む。しかし、パソコン103へのID付録音機器106のチェックイン、チェックアウトには、データの送受信ごとに認証、暗号処理等の手続が必要であることから、ID付録音機器106に高性能な処理回路が必要となっていた。また、認証、暗号処理の負荷が大きく、ユーザが利用しやすいものではなかった。

【0012】本発明の目的は、上記の課題を考慮して、ユーザにとって使い勝手がよい著作権保護システム、著作権保護方法、そのホスト装置、そのプログラム、そのプログラムを担持した媒体を提供することを目的とする。

【0013】

【課題を解決するための手段】上記課題を解決するための、第1の本発明は、所定のコンテンツを所定の暗号化方法で暗号化するとともに、再生を許可された再生装置（5）の台数に応じて、特定の再生装置（5）を選択し、前記選択された特定の再生装置（5）へ、前記暗号化されたコンテンツ（6）を復号化するための復号化情報（7）を送るホスト装置である。

【0014】第2の本発明は、前記選択を指示するための選択指示手段をさらに備える、請求項1に記載のホスト装置である。

【0015】第3の本発明は、前記暗号化は、前記ホスト装置に固有のホストIDを利用したものであり、前記

復号化情報(7)には、前記特定の再生装置(5)の機器IDと、前記ホストIDが含まれている、第1の本発明のホスト装置である。

【0016】第4の本発明は、前記所定のコンテンツおよび前記台数の情報(38)は、配信サーバ(1)から暗号化されて配信されたものである、第1の本発明のホスト装置である。

【0017】第5の本発明は、ホスト装置により暗号化されたコンテンツ(6)が有するホストIDと、前記復号化情報(7)に含まれているホストIDとが一致し、かつ、前記復号化情報(7)に含まれる機器IDと、固有の機器IDとが一致していることを条件として、前記暗号化されたコンテンツ(6)を再生する再生装置であって、前記ホスト装置は、所定のコンテンツを固有のホストIDを利用して暗号化するとともに、再生を許可された再生装置(5)の台数に応じて、特定の再生装置(5)を選択し、前記選択された特定の再生装置(5)へ、前記暗号化されたコンテンツ(6)を復号化するための、前記特定の再生装置(5)の機器IDおよび前記ホストIDが含まれている復号化情報(7)を送る、再生装置である。

【0018】第6の本発明は、前記再生装置(5)は、インターネットに接続されていない、第5の本発明の再生装置である。

【0019】第7の本発明は、所定のコンテンツを配信する配信サーバ(1)と、所定のコンテンツを所定の暗号化方法で暗号化するホスト装置(3)と、前記暗号化されたコンテンツを再生する再生装置(5)と、を備え、前記ホスト装置(3)は、再生を許可された再生装置(5)の台数に応じて、特定の前記再生装置(5)を選択し、前記選択された特定の再生装置(5)へ、前記暗号化されたコンテンツ(6)を復号化するための復号化情報(7)を送り、前記再生装置(5)は、前記送られた復号化情報(7)を利用して、前記暗号化されたコンテンツ(6)を再生する著作権管理システムである。

【0020】第8の本発明は、所定のコンテンツを配信する配信サーバ(1)と、前記所定のコンテンツ(1)を所定の暗号化方法で暗号化するホスト装置(3)と、前記暗号化されたコンテンツを再生する再生装置(5)と、を備える著作権管理システムを利用した著作権管理方法であって、前記ホスト装置(3)は、再生を許可された前記再生装置(5)の台数に応じて、特定の前記再生装置(5)を選択し、前記選択された特定の再生装置(5)へ、前記暗号化されたコンテンツ(6)を復号化するための復号化情報を送り、前記再生装置(5)は、前記送られた復号化情報(7)を利用して、前記暗号化されたコンテンツ(6)を再生する著作権管理方法である。

【0021】第9の本発明は、第7の本発明の著作権管理システムの、所定のコンテンツを所定の暗号化方法で

暗号化するホスト装置(3)と、前記暗号化されたコンテンツ(6)を再生する再生装置(5)と、をコンピュータとして機能させるためのプログラムである。

【0022】第10の本発明は、第9の本発明のプログラムを担持させた記録媒体であって、コンピュータで利用可能な記録媒体である。

【0023】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照しながら説明する。

【0024】図1は、本発明の著作権管理システムの構成の概要を示す図である。図1において、1は電子音楽配信(EMD)サーバであり、2はインターネット回線、3は、本発明のホスト装置の一例である、所定のホストIDを有するユーザ側のパソコン、4はCD-R、5は、本発明の再生装置の一例である、インターネット回線2に接続されていない、個別の所定の機器IDを有する再生機器である。図1においては、再生機器5として機器A、機器B、機器Cが示されており、機器A、機器Cには再生が許可され、機器Bには再生が許可されていない状態を示している。また、それぞれの再生機器5はパソコン3と通信ケーブルで接続可能な構成である。

【0025】次に、このような著作権管理システムの動作の概略を説明する。まず、ユーザは、EMDサーバ1からユーザ側のパソコン3でコンテンツデータをインターネット回線2を介してダウンロードする。パソコン3は、ダウンロードされたコンテンツデータを所定の方法で暗号化してCD-R4にコピーをする。このとき、パソコン3により複数のCD-R4にコピーされてもよいし、作成された1枚のCD-R4が複数のCD-R4にコピーされてもよい。ユーザは、あらかじめ決められている再生機器5である機器Aまたは機器CにCD-R4を挿入する。再生を許可された機器Aまたは機器Cは、所望のコンテンツを再生することができる。このとき、ユーザが再生が許可されていない機器BにCD-R4を挿入しても所望のコンテンツを再生することができない。このように、本発明の著作権管理システムのポイントは、汎用メディアであるCD-R4にコピーされたコンテンツデータは、パソコン3の独自の方式で暗号化され、あらかじめ再生が許可された再生機器5でしか再生できないことである。

【0026】図2は、所定の再生機器5にしかコンテンツデータが再生されないという動作の概要を示す。パソコン3は、ホストIDとしてID001を有している。再生機器5は、機器IDとしてID00Aを有している。そして、パソコン3は、CD-R4に所望のコンテンツデータを所定の方法で暗号化し、ホストIDを利用した暗号化IDであるENC001を付与する。すなわち、CD-R4には、ENC001を有する暗号化されたコンテンツ6が記録されている。パソコン3は、一方で本発明の復号化情報の一例である復号鍵7を生成す

る。この復号鍵7は、暗号化されたコンテンツを復号するためのホストIDを利用して作成された復号用IDであるDEC001、および再生機器5の機器IDであるID00Aを有する。そして、復号鍵7は、パソコン3から再生機器5に送信される。

【0027】ユーザは、暗号化されたコンテンツが収容されたCD-R4を再生機器5に挿入する。再生機器5は、暗号化されたコンテンツに含まれているENC001と復号鍵に含まれているDEC001が対応するか検証する。また、再生機器5は、復号鍵7に含まれている機器ID00Aと、再生機器5に固有の機器IDである機器ID00Aが一致するか検証する。上記の両方の検証において、対応および一致が見られた場合は、再生機器5は、CD-R4に含まれる暗号化されたコンテンツを復号化することにより、所望のコンテンツを再生することができる。

【0028】図3は、パソコン3の構成の一例を示すブロック図である。22は、EMDサーバ1において汎用的な暗号方法により暗号化されたコンテンツの配信をインターネット回線2を介して受けるための通信手段であり、23は、前記通信手段22から暗号化されたコンテンツを取得するためのコンテンツ入手手段であり、8は入手した暗号化されたコンテンツを汎用的な復号方法により復号するための復号手段であり、9は復号化されたコンテンツを暗号化用IDを利用して暗号化するコンテンツ暗号化手段であり、10は暗号化されたコンテンツをCD-R4に記録するための記録手段である。

【0029】14は、ホストIDを保持している自ID保持手段であり、15は自ID保持手段14からホストIDを取得するための自ID取得手段であり、16は取得したホストIDから暗号用IDおよび復号用IDを生成するための暗号用ID復号用ID生成手段であり、17は、暗号用ID復号用ID生成手段16により生成されたID、および機器ID入手手段20により生成されたIDを利用して復号鍵を生成するための復号鍵生成手段であり、18は、復号鍵生成手段17により生成された復号鍵を再生機器5に発行するための復号鍵発行手段である。

【0030】11は、通信手段22を介して1から台数情報38（後述）を入手するための鍵入手手段であり、13は、鍵管理情報制御手段であり、12は、鍵管理情報データベースである。

【0031】19は、再生機器5と通信するための通信手段であり、20は、通信手段19を介して再生機器5から機器IDを入手するための機器ID入手手段であり、21は再生機器5に発行された復号鍵を削除するための復号鍵削除手段である。

【0032】上記の暗号用ID復号用ID生成手段16、復号鍵生成手段17、復号鍵発行手段18、および復号鍵削除手段21は、本発明の選択指示手段の一例と

して対応する。

【0033】図4は、再生機器5の構成の一例を示すブロック図である。図4において、24は、CD-R4を駆動するためのメディアドライブであり、25は、メディアドライブ24にセットされたCD-R4に記録されたコンテンツから暗号用IDを抽出するための暗号用ID抽出手段であり、26はパソコン3と通信するための通信手段であり、27はパソコン3により発行された復号鍵7を保持しておくための復号鍵保持手段であり、28は通信手段26または復号鍵保持手段27から復号鍵7を取得するための復号鍵取得手段であり、37は復号鍵取得手段28から復号用IDを抽出するための復号用ID抽出手段であり、30は復号鍵取得手段28において取得した復号鍵7から機器IDを抽出するための機器ID抽出手段であり、31は各再生機器5に固有の機器IDを保持するための機器ID保持手段であり、33は機器ID取得手段32において取得された機器IDと機器ID抽出手段30において抽出された機器IDとを比較するための機器ID比較手段である。

【0034】34は暗号・復号用ID比較手段29および機器ID比較手段33における比較結果より、所望のコンテンツを再生機器5において再生することが可能であるかどうかを判定する再生可否判定手段であり、35は再生可否判定手段34における判定結果に基づいて、メディアドライブ24から供給される暗号化されたコンテンツデータを復号するための復号処理手段であり、36は復号処理手段35において復号処理されたコンテンツを再生出力するための出力手段である。

【0035】次に、以上の構成の本発明の著作権管理システムの動作の詳細を図5および図6を参照しながら説明する。図5は、著作権管理システム全体における動作を説明する図である。また図6は、本発明の著作権管理システムの全体のフロー図である。

【0036】まず、ユーザは、台数情報38の配信をインターネット回線2を介して要求する。すなわちEMDサーバ1側にサービスへの入会を要求する（ステップ101）。この要求には、ユーザが希望する再生機器5の再生許可台数の情報が含まれている。EMDサーバ1において、ユーザの加入を認める場合は、台数情報38をインターネット回線2を介して配信する（ステップ102）。この台数情報38の中には、入会を希望する個別のユーザの再生許可台数が含まれている。

【0037】そして、ユーザがコンテンツの配信を希望する場合は、パソコン3は所望のコンテンツの配信要求をEMDサーバ1にインターネット回線2を介して送信する（ステップ103）。EMDサーバ1はコンテンツ配信要求を受けると、ユーザが所望するコンテンツを汎用的な暗号方法で暗号化したコンテンツデータおよび台数情報38をパソコン3にインターネット回線2を介して送信する（ステップ104）。パソコン3は暗号化さ

れたコンテンツデータおよび台数情報38を受けると、汎用的な復号方法により暗号化されたコンテンツデータおよび台数情報38を復号する。

【0038】ユーザによりCD-R4がパソコン3にセットされ所定の操作がされると、パソコン3は復号化されたコンテンツをホストIDを利用して暗号化し、CD-R4に記録する(ステップ105)。

【0039】そして、ユーザが暗号化されたコンテンツが記録されたCD-R4を再生機器5において再生する場合、再生機器5は、まず復号鍵7の発行要求を行う(ステップ106)。なお、再生機器5が復号鍵7を有している場合、および、パソコン3から再生機器5に対してトリガをかける場合は、このステップ106は不要となる。

【0040】パソコン3は、復号鍵7の発行要求を再生機器5から受けると、再生機器5に対して再生機器5の機器IDの送信要求を出す(ステップ107)。再生機器5が機器IDの送信要求を受けると、再生機器5はその再生機器5に固有の機器IDをパソコン3に送る(ステップ108)。そして、パソコン3は、パソコン3に固有のホストIDから生成された復号用IDであるDEC001と再生機器5に固有の機器IDであるID00Aとから復号鍵7を生成する。そしてパソコン3は、生成された復号鍵7を再生機器5に送る(ステップ109)。

【0041】ユーザが所望のコンテンツを再生機器5において再生しようとする場合は、再生機器5はCD-R4に対して暗号化コンテンツの再生要求を出す(ステップ110)。再生機器5においては、CD-R4の暗号化されたコンテンツ6に記録されたENC001とパソコン3から送信された復号鍵7に含まれるDEC001とを比較し、両者が対応するものであることを検証する。すなわち、両者においてホストIDである001が一致することを検証する。さらに、再生機器5は復号鍵7に含まれる機器IDであるID00Aと再生機器5に固有の機器IDであるID00Aとが一致するかを検証する。そして、上記の両方の条件が満たされることが確認されると、再生機器5は、暗号化されたコンテンツ6を復号化し、所望のコンテンツを再生する(ステップ111)。

【0042】図5において、中央部の囲まれた部分は、EMDサーバ1とパソコン3とのデータのやり取りを行うための専用ソフトにおける処理を示す。また同図における右下方において囲まれた部分は、再生機器5とパソコン3との間のデータのやり取りを行うための専用ソフトにおける処理を示す。これらの専用ソフトでは、鍵などのデータを外部からアクセスされることがないように保護しながら処理が行われているため、送受信した情報が外部に漏洩することはない。

【0043】図7は、上記の著作権管理システムにおい

てパソコン3の動作を説明したフロー図である。図3および図7を参照しながらパソコン3の動作を次に説明する。

【0044】図7(a)は、所望のコンテンツデータをCD-R4にコピーするときのフローである。ユーザは、まずパソコン3の動作を開始する(ステップ210)。そしてパソコン3は、ユーザに台数情報38を新規購入するかどうかの決定を促す(ステップ211)。台数情報38を購入すると判断する場合は、パソコン3は台数情報38の購入処理をし(ステップ212)、パソコン3の鍵管理情報制御手段13は鍵管理情報データベース12に鍵管理情報を登録する(ステップ213)。台数情報38がすでに存在して新規購入する必要がない場合は、次のステップに進む。

【0045】ステップ213において、鍵管理情報が登録されると、パソコン3は次にコンテンツを購入するかどうかの決定をユーザに促す(ステップ214)。コンテンツが購入されることが決定されると、パソコン3のコンテンツ入手手段23は通信手段22を介してコンテンツの購入処理を行う(ステップ215)。コンテンツが購入されないと決定された場合は、処理を終了する(ステップ218)。ステップ215においてコンテンツ購入処理が完了すると、復号手段8は暗号化されているコンテンツを汎用的復号方法により復号化する。そして、コンテンツ暗号化手段9は、暗号用ID復号用ID生成手段16により生成された暗号用IDを用いてコンテンツを暗号化し(ステップ216)、記録手段10は暗号化されたコンテンツをCD-R4にコピーして(ステップ217)、処理を終了する(ステップ218)。

【0046】図7(b)は、再生許可された再生機器5に対してパソコン3が復号鍵を生成するときのフローである。まず、パソコン3は復号鍵の発行処理を開始させる(ステップ220)。そしてパソコン3は、再生機器5から復号鍵7を取得する指示を出す(ステップ221)。次にパソコン3は再生機器5が復号鍵7を有しているかどうかを検証する(ステップ222)。再生機器5がすでに復号鍵7を有している場合は、復号鍵7を削除するかどうかを判断する(ステップ223)。復号鍵7を削除しない場合は、処理を終了する(ステップ230)。再生機器5が復号鍵7を有していない場合は、パソコン3は次のステップに進む。次のステップにおいて鍵管理情報制御手段13は鍵管理情報データベース12から鍵管理情報を入手し(ステップ225)、復号鍵生成手段17に渡す。

【0047】一方、機器ID入手手段20は、通信手段19を介して再生機器5から機器IDを取得し(ステップ226)、復号鍵生成手段17は復号鍵7の発行が適切であるかどうかを判断する(ステップ227)。もし、復号鍵7の発行が適切でない場合は処理を終了する(ステップ230)。復号鍵7の発行が適切である場合

は、復号鍵生成手段17は暗号用ID復号用ID生成手段16から得た復号用IDと再生機器5から取得した機器IDから復号鍵7を生成する(ステップ228)。そして復号鍵発行手段18は復号鍵7を再生機器5に送信して(ステップ229)処理を終了する(ステップ230)。

【0048】図7(c)は、鍵管理情報データベース12に格納されている鍵管理情報の一例を示す。この鍵管理情報は、ユーザはEMDサーバ1から3台の再生許可台数を得ており、ID00AのIDを有する再生機器5の1台に復号鍵7を発行している状況を示している。また、この鍵管理情報には、鍵の入手日と復号鍵7の発行日とが記録されている。

【0049】図8は、再生機器5側における処理フローを示す。図8(a)におけるステップ341～ステップ344は、図6におけるステップ106～ステップ109に対応する。図8および図4を参照しながら次に再生機器5の動作フローを説明する。

【0050】図8(a)において、再生機器5はまず復号鍵要求の処理を開始する(ステップ340)。通信手段26は復号鍵7の発行要求をパソコン3側に送信する(ステップ341)。パソコン3側から再生機器5の機器IDの送信が要求されると、復号鍵取得手段28は機器ID保持手段31に保持されている機器IDを通信手段26を介してパソコン3側に送信する(ステップ342)。パソコン3から復号鍵が発行されると、通信手段26は発行された復号鍵7を受信し(ステップ343)、復号鍵取得手段28は取得した復号鍵7を復号鍵保持手段27に登録し(ステップ344)、処理を終了する(ステップ345)。

【0051】図8(b)は、再生機器5においてコンテンツを再生する際の動作フロー図である。

【0052】まず、再生機器5はユーザの操作によりコンテンツ再生処理を開始する(ステップ350)。復号鍵取得手段28は復号鍵保持手段27が復号鍵7を所持しているかどうかを確認する(ステップ351)。復号鍵保持手段27に復号鍵7が存在しない場合は、復号鍵7を取得するかどうかのステップに進む(ステップ352)。このステップ352において、復号鍵7を取得しない場合は処理を終了し(ステップ361)、復号鍵7を取得する場合は、図8(a)に示す復号鍵要求フローに進む(ステップ353)。復号鍵保持手段27に復号鍵7が存在する場合は、復号鍵7に含まれる機器IDと再生機器5の機器IDとを比較する(ステップ354)。すなわち機器ID抽出手段30は、復号鍵取得手段28に存在する復号鍵7から機器IDを抽出し、機器ID比較手段33に渡す。また、機器ID取得手段32は、機器ID保持手段31に存在する固有の機器IDを取得し機器ID比較手段33に渡す。そして機器ID比較手段33は、機器ID抽出手段30から渡された機器

IDと機器ID取得手段32から渡された機器IDとが一致するかどうかを比較する(ステップ355)。もし、両者の機器IDが一致しない場合は処理を終了する(ステップ361)。

【0053】両者の機器IDが一致する場合は、暗号用ID抽出手段25は、メディアドライブ24からコンテンツに含まれる暗号用IDを取得して(ステップ356)、暗号・復号用ID比較手段29に渡す。一方、復号用ID抽出手段37は復号鍵取得手段28に存在する復号鍵7から復号用IDを抽出して暗号・復号用ID比較手段29に渡す。そして暗号・復号用ID比較手段29は、暗号化されたコンテンツから取得した暗号用IDと復号鍵7に含まれる復号用IDとを比較する(ステップ357)。すなわち、暗号・復号用ID比較手段29は、暗号用IDと復号用IDとを比較し、両者が同じホストIDに対応するものであるかどうかを検証する(ステップ358)。

【0054】上記の暗号用IDと復号用IDとが対応しない場合は再生可否判定手段34は再生不可である判定をして処理を終了する(ステップ361)。両者のIDが対応するものである場合は、再生可否判定手段34は再生が可能である判定を出し、復号処理手段35は、暗号化されたコンテンツ6を復号鍵7を利用して復号化し(ステップ359)、出力手段36は復号化されたコンテンツを出力することによりユーザが所望するコンテンツを再生し(ステップ360)、処理を終了する(ステップ361)。

【0055】図9は、再生許可された再生機器5が複数台ある場合の、本発明の著作権管理システムの全体を示す模式図である。図9に示す例においては、再生機器5のうち、ポータブルCDプレーヤである機器Aと、ミニコンボである機器Bの2台が再生許可を受けている場合を示している。このような場合、パソコン3は機器Aに復号用IDとしてDEC001と、機器IDとしてID00Aとを有する復号鍵7を生成し、機器Bに復号用IDとしてDEC001と機器IDとして00Bとを有する復号鍵7を生成する。そしてこれらの復号鍵7はそれぞれ機器Aおよび機器Bに送信されている。

【0056】ここで、暗号化されたコンテンツ6を、機器Aで再生するため、および機器Bで再生するためにCD-R4は、パソコン3において2枚コピーされる。このときそれぞれのCD-R4には、同一の暗号化されたコンテンツ6が記録されている。すなわち、暗号化されたコンテンツ6には、同一の暗号化されたコンテンツデータとともに暗号用鍵としてENC001が格納されている。

【0057】機器A、および機器Bは、それぞれが有している復号鍵7で暗号化されたコンテンツ6を復号化して所望のコンテンツを再生する。

【0058】図10は、以上までの構成、動作による本

発明の著作権管理システムにより、著作権が保護されるバリエーションを図示する。

【0059】図10においては、ホスト装置として、パソコン3とは異なる別のパソコン43が存在する場合を示している。また、再生機器5として機器A、機器B、機器Cの三台が存在し、このうち機器Aがパソコン3により復号鍵7が発行された再生機器5である状態を示している。

【0060】上記のような条件において、まず、第三者のパソコンであるパソコン43でコンテンツが記録されたCD-Rを不正入手した場合を考える。この場合、パソコン43はパソコン43に挿入されたCD-R4にパソコン43のホストIDであるID002を利用してコンテンツを暗号化し、暗号化されたコンテンツ46には暗号鍵としてENC002が含まれている。ユーザが機器Aを使用して所望のコンテンツを再生しようとする、CD-R4が暗号化されたコンテンツ46を有している場合、すなわち、暗号化されたコンテンツ46にENC002が存在する場合、機器Aは、上述のように、機器Aが有する復号鍵7に含まれる復号用IDであるDEC001と、暗号化されたコンテンツ46に含まれるENC002とを比較し、両者は同一のホストIDに由来しないことを確認する。従って機器Aは、このようにパソコン43で記録されたCD-Rを不正に入手することによって得たコンテンツを再生することができない。

【0061】次に、機器Bには復号鍵7が発行されていないとすると、機器Bは、当然ながらパソコン3によりコピーされたコンテンツもパソコン43によりコピーされたコンテンツも再生することができない。

【0062】次に、機器Cは、正規の復号鍵7を有しておらず、機器Aの復号鍵7を不正にコピーしたものを有しているとする。その場合、機器Cが有する固有の機器IDはID00Cであり、一方で不正コピーされた復号鍵7に存在する機器IDは、ID00Aであるので、機器Cは、両者の機器IDが一致しないと判断する。従って、復号鍵7を不正コピーした機器Cでは、所望のコンテンツを再生することはできない。もちろん、パソコン43により不正コピーしたコンテンツを再生することもできない。

【0063】図11は、以上のように場合において、著作権が保護される範囲を一覧にした図である。すなわち、再生機器5が再生許可された正規の復号鍵7を有する機器であり、CD-R4がユーザの正規のパソコン3によりコピーされた場合にのみ、ユーザが所望するコンテンツを再生することができる。しかし、再生機器5が復号鍵7を有さない機器である場合、および再生機器5が復号鍵7を不正コピーしている機器である場合は、そのようなコンテンツを再生することができない。

【0064】図12は、再生機器5の再生許可台数を変更しないで再生許可された再生機器5を変更するときの

フローを示す図である。

【0065】例えば、ユーザが三台の再生機器5、すなわち機器A、機器B、機器Cを有しており、このうち機器Aおよび機器Bの二台に再生許可がなされているものとする。そして、ユーザは二台という再生許可台数は変更しないで、再生許可機器を、機器Aおよび機器Bから、機器Bおよび機器Cに変更する場合を例としてその場合の本実施の形態の著作権管理システムの動作を以下に説明する。

【0066】図12において、ステップ401は図6に示すステップ101～ステップ104に対応する。また、ステップ402は図6に示す105に対応し、ステップ403～ステップ406は図6に示すステップ106～ステップ109に対応する。また、ステップ407～ステップ410は、ステップ403～ステップ406に対応する動作がパソコン3と機器Bとの間でなされたものである。ここまで動作がなされている状態で、機器A、および機器Bは、ユーザが所望するコンテンツを再生することができる（ステップ411、ステップ412）。しかし、復号鍵7を有していない機器Cは、コンテンツを再生することができない（ステップ413）。

【0067】次に、パソコン3は機器Aに、機器Aが有する復号鍵7を送信するよう送信要求を出す（ステップ414）。そして、機器Aは、パソコン3から復号鍵7の送信要求を受けると、パソコン3に機器Aが有する復号鍵7を送信し、機器Aから復号鍵7を削除する（ステップ415）。また、パソコン3においても受け取った機器Aの復号鍵7を復号鍵削除手段21により削除する（ステップ224（図7（b）参照））。

【0068】そして、機器Cとパソコン3との間では、ステップ416～ステップ419において、ステップ403～ステップ406と同様の処理により、復号鍵7が機器Cに送信される。その結果、機器Aでは所望のコンテンツを再生することができず（ステップ420）、機器Bおよび機器Cにおいて所望のコンテンツを再生することができる（ステップ421、422）。

【0069】以上のように、本実施の形態の携帯の著作権管理システムによれば、所望のコンテンツを汎用のCD-R4に複数枚コピーが可能であるので、ポータブルプレーヤ、ミニコンボ、カーステレオ等、複数の再生機器5で再生する場合、それぞれの再生機器5にセットしておくことができ、いちいちCD-R4を持ち運ぶ手間をかけなくてもよい。

【0070】本実施の形態の著作権管理システムによれば、CD-R4の複製を制限するものではなく、再生される再生機器5の台数を制限することにより、著作権の保護を図りつつもユーザの利便性を向上させることができる。

【0071】また、EMDサーバ1は、個別の再生機器5のライセンス管理を行う必要がなく、再生機器5の使

用許可台数のみを管理すればよいので、E M Dサーバ1側にとっても簡単なシステム構成で済む。

【0072】また、所望のコンテンツを復号するための復号鍵7は、ユーザ側のパソコン3において発行されるので、ユーザはいちいちE M Dサーバ1側に問い合わせる必要がなく、簡単な処理で所望のコンテンツを楽しむことができる。

【0073】なお、以上までの説明は、本発明の著作権管理システムに関するものであるが、上記の構成のシステムを利用した著作権管理方法も本発明の範囲である。

【0074】また、以上までの説明において、ステップ101におけるE M Dサーバ1からパソコン3への台数情報38の配信は、インターネット回線2を介してなされたとしたが、例えば郵便等のほかの方法で送信または送付されてもよい。

【0075】また、以上までの説明では、パソコン3と再生機器5は通信ケーブルで接続されて復号鍵7のやりとり等がなされたとしたが、パソコン3と再生機器5は有線ではなく無線で接続される構成であってもよい。さらには、C D - R等の物理的なメディアを利用して復号鍵7のやりとり等がなされる構成であってもよい。その場合は、パソコン3と再生機器5との間の復号鍵7等のやりとりは送信または受信ではなく、送られ、または受け取られる動作となる。そのような場合も上記と同様の効果を得ることができる。

【0076】また、以上までの説明では、暗号化されたコンテンツが記録されるメディアは、C D - Rであるとしたが、他のメディアであっても当然よい。

【0077】また、以上までの説明では、パソコン3は、再生許可された台数以内の再生機器5に復号鍵7を発行するとしたが、さらに特定の機器に復号鍵7の発行を制限する機能があってもよい。そのような例として、例えば、高音質対応の再生機器5にのみ復号鍵7を発行する構成であってもよい。

【0078】また、以上までの説明におけるコンテンツには、音楽データのみならず、静止画像データ、動画データ、文字データ、その他の情報も含まれる。すなわち、本発明の配信サーバは、E M Dサーバ1に限定されず、上記のようなさまざまなコンテンツを配信することができるサーバであってもよい。

【0079】また、以上までの説明では、本発明のホスト装置は、パソコン3、43であるとしたが、本発明のホスト装置は上記の機能を果たすことができればパソコン以外の機器であってもよい。そのような例としては例えば携帯電話、携帯端末等が挙げられるがこれらに限定されない。

【0080】また、以上までの説明では、再生機器5は一台または三台である例を説明したが、再生機器5が再生許可台数以内であれば何台であってもよいことは言うまでもない。また、再生許可台数を変更したい場合は、

図6に示すステップ101において再生許可台数の変更を配信サーバ側に通知すればよい。

【0081】また、本発明のプログラムは、上述した本発明の著作権管理システムの全部又は一部の手段（又は、装置、素子等）の機能をコンピュータにより実行させるためのプログラムであって、コンピュータと協働して動作するプログラムである。

【0082】又、本発明の記録媒体は、上述した本発明の著作権管理システムの全部又は一部の手段（又は、装置、素子等）の全部又は一部の機能をコンピュータにより実行させるためのプログラムを担持した記録媒体であり、コンピュータにより読み取り可能且つ、読み取られた前記プログラムが前記コンピュータと協働して前記機能を実行する記録媒体である。

【0083】尚、本発明の上記「一部の手段（又は、装置、素子等）」とは、それらの複数の手段の内の、一つ又は幾つかの手段を意味し、本発明の上記「一部のステップ（又は、工程、動作、作用等）」とは、それらの複数のステップの内の、一つ又は幾つかのステップを意味する。

【0084】又、本発明の上記「手段（又は、装置、素子等）の機能」とは、前記手段の全部又は一部の機能を意味し、本発明の上記「ステップ（又は、工程、動作、作用等）の動作」とは、前記ステップの全部又は一部の動作を意味する。

【0085】又、本発明のプログラムの一利用形態は、コンピュータにより読み取り可能な記録媒体に記録され、コンピュータと協働して動作する態様であっても良い。

【0086】又、本発明のプログラムの一利用形態は、伝送媒体中を伝送し、コンピュータにより読みとられ、コンピュータと協働して動作する態様であっても良い。

【0087】又、本発明のデータ構造としては、データベース、データフォーマット、データテーブル、データリスト、データの種類などを含む。

【0088】又、記録媒体としては、ROM等が含まれ、伝送媒体としては、インターネット等の伝送媒体、光・電波・音波等が含まれる。

【0089】又、上述した本発明のコンピュータは、CPU等の純然たるハードウェアに限らず、ファームウェアや、OS、更に周辺機器を含むものであっても良い。

【0090】尚、以上説明した様に、本発明の構成は、ソフトウェア的に実現しても良いし、ハードウェア的に実現しても良い。

【0091】

【発明の効果】本発明によれば、ユーザにとって使い勝手がよい著作権保護システム、著作権保護方法、そのホスト装置、そのプログラム、そのプログラムを担持した記録媒体を提供することができる。

【図面の簡単な説明】

【図 1】図 1 は、本発明の実施の形態の著作権管理システムの概要を示す図である。

【図 2】図 2 は、本発明の実施の形態の著作権管理システムの動作の概要を示す図である。

【図 3】図 3 は、本発明の実施の形態の著作権管理システムを構成するパソコンの構成を示すブロック図である。

【図 4】図 4 は、本発明の実施の形態の著作権管理システムを構成する再生機器の構成を示すブロック図である。

【図 5】図 5 は、本発明の実施の形態の著作権管理システムの全体の動作を示す概略図である。

【図 6】図 6 は、本発明の実施の形態の著作権管理システムの全体の動作を示すフロー図である。

【図 7】図 7 は、本発明の実施の形態の著作権管理システムを構成するパソコンの動作を示すフロー図である。

【図 8】図 8 は、本発明の実施の形態の著作権管理システムを構成する再生機器の動作を示すフロー図である。

【図 9】図 9 は、本発明の実施の形態の著作権管理システムの全体の動作を示す概略図である。

【図 10】図 10 は、本発明の実施の形態の著作権管理システムにより保護される著作権のバリエーションを示す図である。

【図 11】図 11 は、本発明の実施の形態の著作権管理システムにより保護される著作権のバリエーションを示す図である。

【図 12】図 12 は、本発明の実施の形態の著作権管理システムを構成する再生機器の再生許可台数変更する際の動作を示すフロー図である。

【図 13】図 13 は、従来技術の著作権管理システムの概略図である。

【図 14】図 14 は、従来技術の著作権管理システムの概略図である。

【符号の説明】

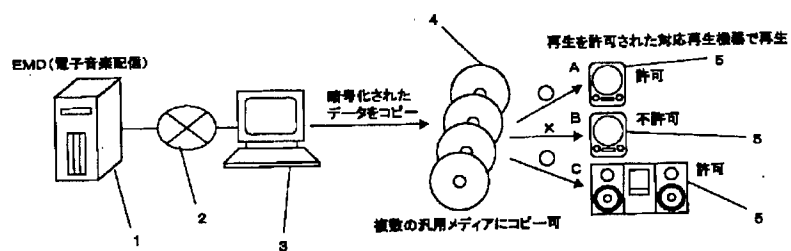
1 EMDサーバ

2 インターネット回線
3、4 3 パソコン
4 C D-R
5 再生機器
6 暗号化されたコンテンツ
7 復号鍵
8 復号手段
9 コンテンツ暗号化手段
10 記録手段
11 鍵入手手段
12 鍵管理情報データベース
13 鍵管理情報制御手段
14 自ID保持手段
15 自ID取得手段
16 暗号用ID復号用ID生成手段
17 復号鍵生成手段
18 復号鍵発行手段
19、22、26 通信手段
20 機器ID入手手段
21 復号鍵削除手段
23 コンテンツ入手手段
24 メディアドライブ
25 暗号用ID抽出手段
27 復号鍵保持手段
28 復号鍵取得手段
29 暗号符号用ID比較手段
30 機器ID抽出手段
31 機器ID保持手段
32 機器ID取得手段
33 機器ID比較手段
34 再生可否判定手段
35 復号処理手段 36 出力手段
37 復号用ID抽出手段
38 鍵

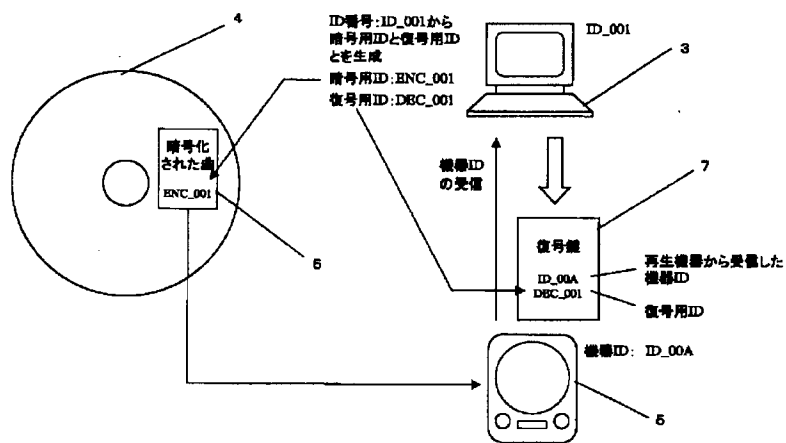
【図 11】

再生機器	暗号機器	暗データ中の 暗号用ID	復号鍵中の 復号用ID	再生機器の 機器ID	復号鍵中の 機器ID	再生の可否	備考
機器A	PC1	ENC_001	DEC_001	ID_00A	ID_00A	○	正解の再生
機器A	PC2	ENC_002	DEC_001	ID_00A	ID_00A	×	未知のPCで暗号化されたデータを不正入手した場合
機器B	PC1	ENC_001	—	ID_00B	—	×	再生機器に復号鍵がない場合
機器B	PC2	ENC_002	—	ID_00B	—	×	再生機器に復号鍵がない場合
機器C	PC1	ENC_001	DEC_001	ID_00C	ID_00A	×	復号鍵を不正入手した場合
機器C	PC2	ENC_002	DEC_001	ID_00C	ID_00A	×	復号鍵を不正入手した場合

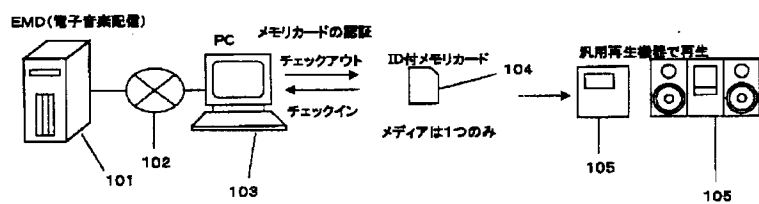
【図1】



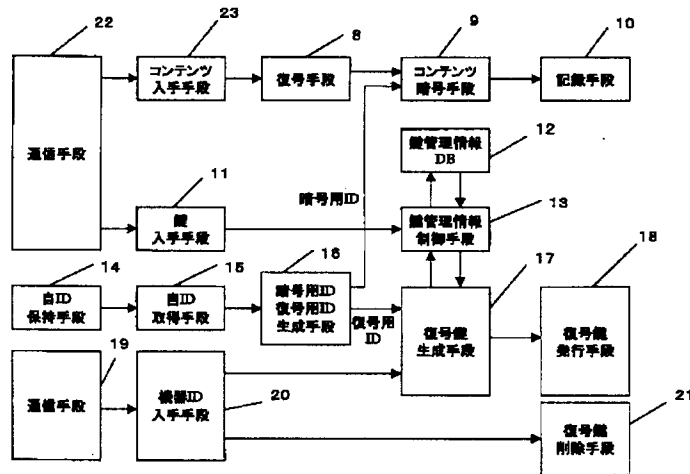
【図2】



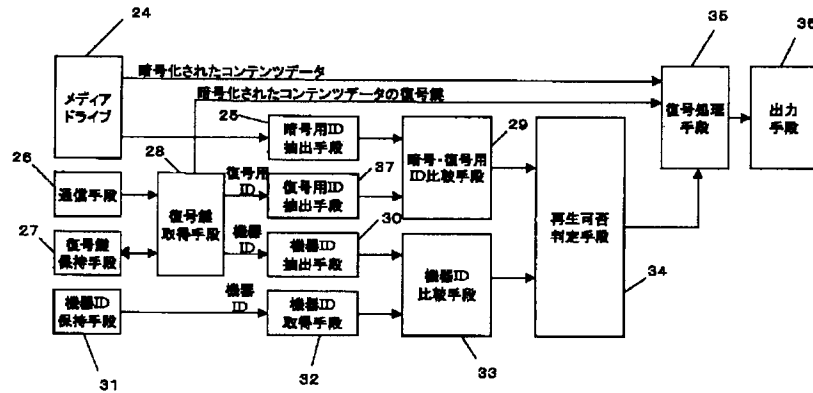
【図13】



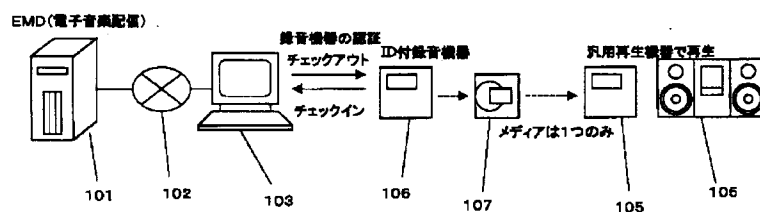
【図3】



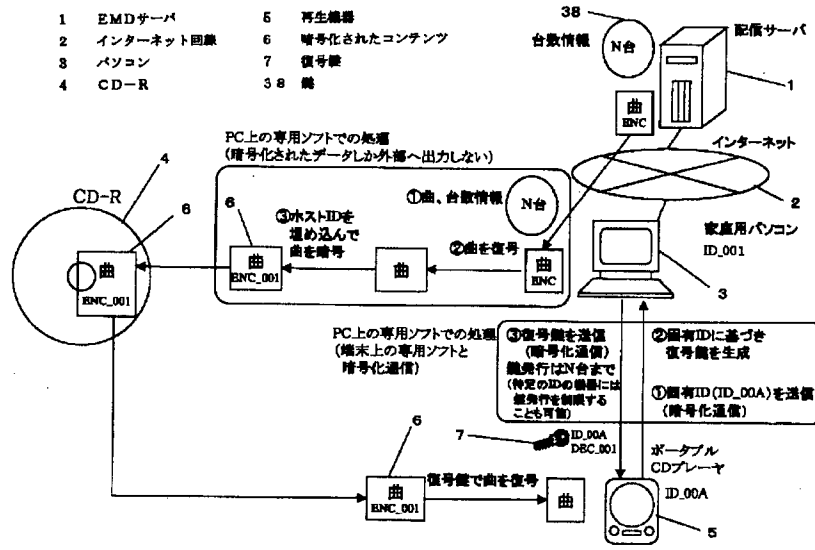
【図4】



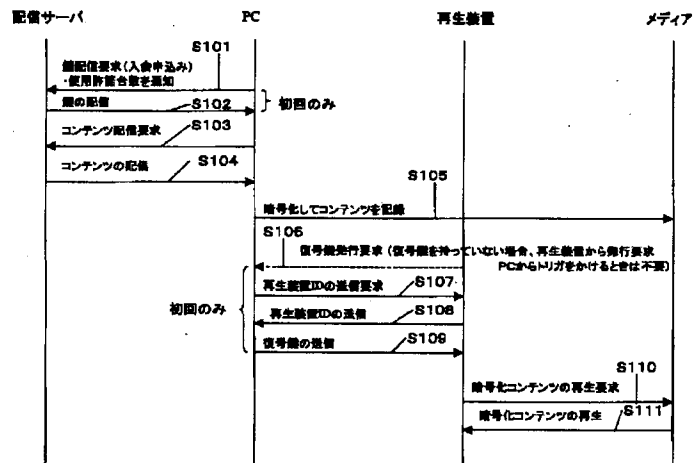
【図14】



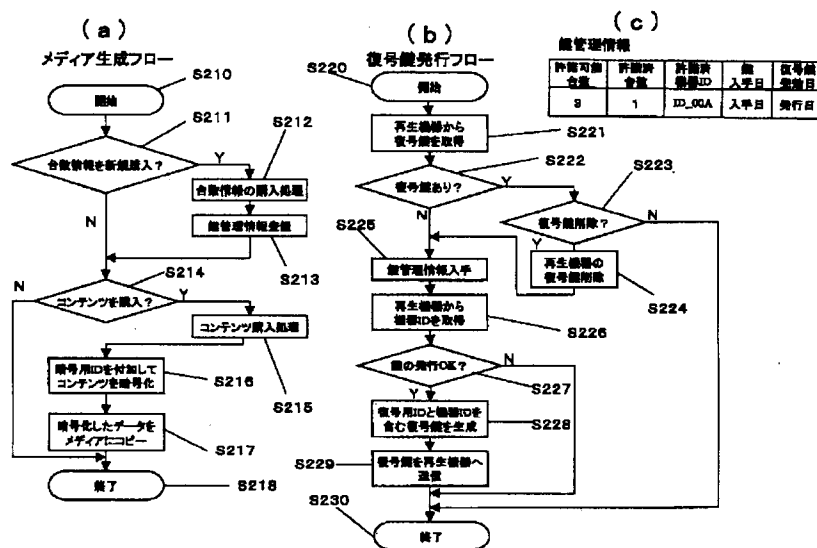
【図5】



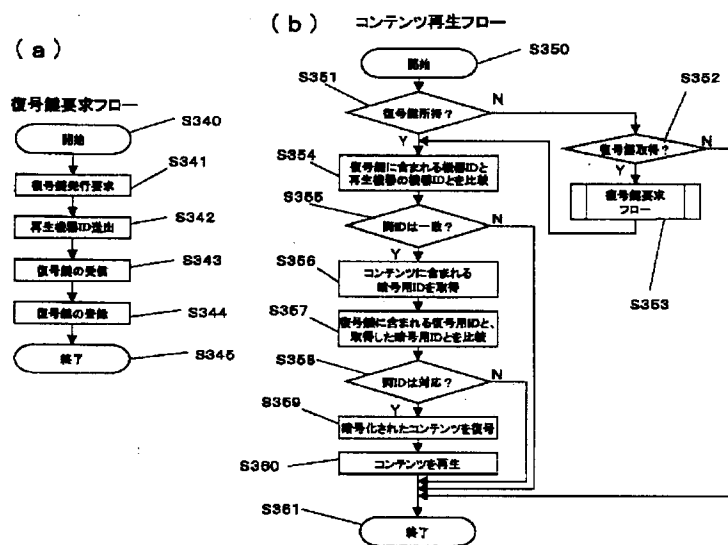
【図6】



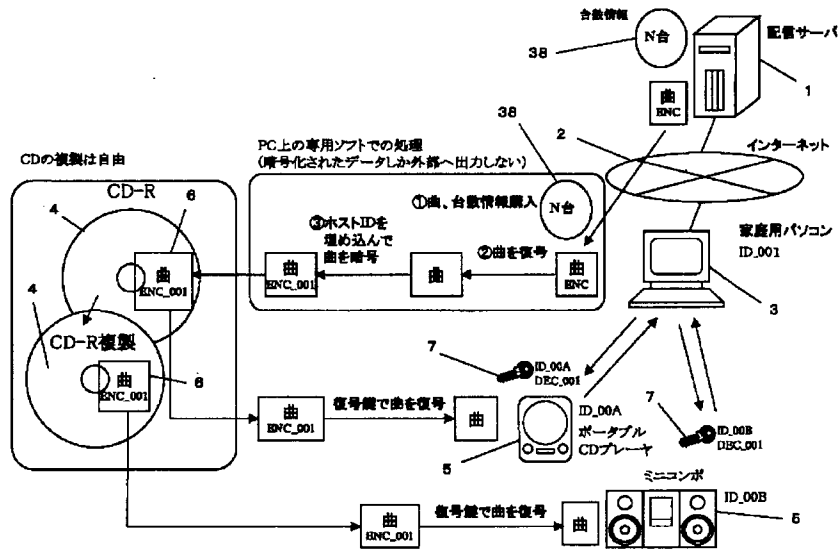
【図 7】



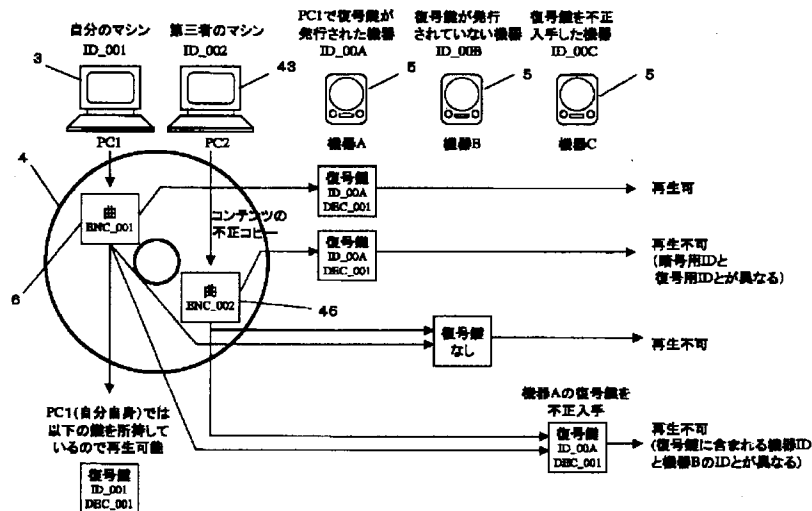
【图8】



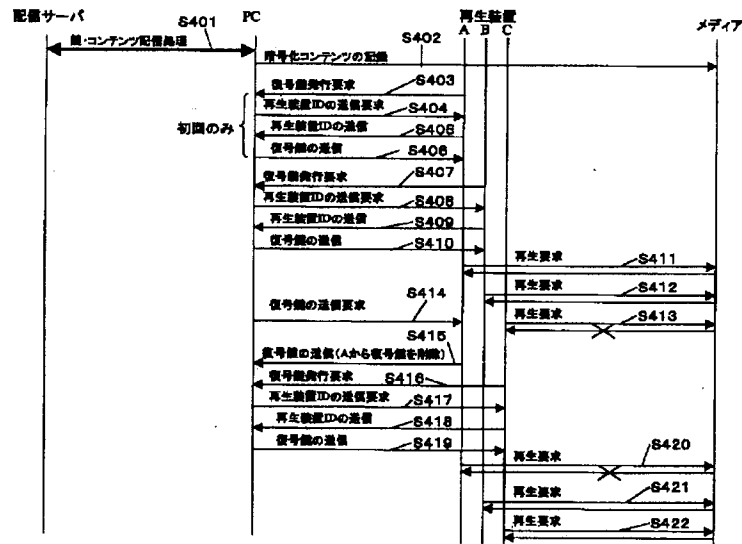
【図9】



【図10】



【図12】



フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	ターム (参考)
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 D
9/32			6 0 1 E
			6 7 3 B

F ターム (参考) 5B017 AA06 BB10 CA16
5D044 AB05 BC05 DE50 GK12 GK17
HL08 HL11
5D110 AA16 AA27 BB01 BB25 BB29
DA08
5J104 AA12 AA16 EA01 EA04 EA18
JA03 KA02 KA15 MA05 NA02
PA07 PA14